RBJ RBJ.NET ROCHESTER BUSINESS JOURNAL
VOLUME 37 NUMBER 37 ■ Part of the BRIDGETOWER MEDIA network ■ FEBRUARY 11, 2022

Data privacy and security concerns with rise of online betting, gaming

VIEWPOINT
Anna Mercado Clark

As of January 8, 2022, New York State joined the ranks of more than a dozen states that have legalized online and mobile sports betting since the U.S. Supreme Court's 2018 decision in Murphy v. National Collegiate Athletic Association, which struck down the Professional and Amateur Sports Protection Act, also known as the Bradley Act. This paved the way for individual states to regulate sports betting, which had effectively been banned nationwide with limited exceptions. According to various analysts, the New York market alone is expected to exceed $1 billion in annual revenue. Indeed, New York State Governor Kathy Hochul has reported that during the first weekend of betting, the four authorized operators received $150 million in wagers from over 650,000 unique user accounts originating from more than 17 million confirmed geolocations. The sheer volume of individual users and bets gives rise to data privacy and security concerns for individuals, employers and companies who wish to participate in this online gaming economy.

Privacy and security issues

Privacy, or freedom from unauthorized intrusion, generally refers to the right or ability to limit how certain information may be collected, accessed or used, and by whom. The online collection of personal information necessarily raises privacy concerns including, but not limited to, the scope and reasonableness of data collection, timing and content of notice provided to users about data collection, how information is used and with whom it is shared, how long it is kept, and what rights individuals have regarding that data. Given that these mobile sports bets are exclusively online transactions, the privacy of children (depending on the law, generally under the age of 18, well below the 21-year-old threshold to place bets legally) is of particular importance.

The proliferation of online betting services, high user utilization, and the commonplace overlap between work and personal devices and networks also raises concerns about the potential for accidental or unauthorized loss of information or funds, and unauthorized intrusion that can result in the loss of integrity or lack of accessibility to essential information, devices or networks.

How to safeguard against risks

There are many ways that individuals, employers and online betting service providers can minimize privacy and security risks. Below are some examples.

Individuals

Novel services can be a target for fraudulent activity. Users should be discerning about the platforms that they download, visit, or use and should use only those platforms that are reputable and have been vetted and approved by regulators. Fraudulent websites and applications can trick users into providing credentials, financial information or funds, which are often irretrievable. Even when using reputable platforms, users should carefully review privacy policies and terms and conditions to know how their information is collected and shared, as well as how they may exercise their rights, which may include accessing or requesting corrections to or deletion of their own personal information. If a user does not agree, they may refuse to consent to provide their information and/or choose another provider. Users should also consider consenting only to the collection

of information that is necessary to complete the particular betting transaction and avoid connecting accounts to debit or checking accounts on an ongoing basis. Individual payments should be made for each transaction from a credit card or similar account instead.

As a matter of digital hygiene, users should avoid using repeat passwords. Activation of multifactor authentication, if available, can further protect online accounts even when a password is compromised.

For betting platforms that allow social networking, users should carefully review their connections and communications to avoid falling victim to social engineering, which occurs when a malicious actor pretends to be a trusted contact and manipulates a user into divulging private information.

Employers

Work-from-home arrangements may be the norm for the foreseeable future. As a result, the divide between personal and professional devices and networks could continue to erode. Accordingly, employees' online activities, including the use of websites and applications for online betting, can be a source of security vulnerabilities. Employers should consider educating employees regularly regarding risks, the evolving threat landscape, and best practices, while employing administrative and technical measures to improve employees' (and, by extension, the organization's) security postures. This may include implementing policies regarding passwords, device use, network access, minimum software requirements, and security settings among other things. Remote mobile device management software can be used to manage assets on an employee's phone, tablet or laptop, in case these are compromised. Network monitoring software can also allow employers to identify unauthorized intrusions, and provide an up-to-date and tested incident response policy can facilitate a swift response.

In addition, online betting can have a number of negative impacts on the workplace, including reducing productivity, increasing absences and, in some cases, leaving a company vulnerable to theft and fraud. Employers should consider adopting policies that, among other things: (1) prohibit or restrict gambling during working hours and/or on employer-owned resources; and (2) notify employees that they may be subject to monitoring and to have no expectation of privacy when utilizing employer-owned resources.

Online betting operators and third-party service providers

Online betting operators and their third-party service providers (such as to facilitate payment) should identify and comply with relevant laws, regulations, and even informal guidance from state or federal regulators. These may not be limited to gambling authorities because data protection laws frequently overlap.

Privacy policies and terms and conditions should be regularly updated, readily accessible and provide sufficient information to users as may be required by law or industry standards. Operators may ultimately be responsible even for information collected by a third party on its behalf.

Data collection should be scaled to what is necessary or reasonable given the notice provided to users, the transaction and the security measures that the operator employs. Reasonable steps should be taken to prevent the collection of children's data. Data should be deleted as soon as it is no longer legally required or needed for business purposes.

Service providers should be vetted and have appropriate contractual and insurance protections in place.

Just as with any organization, online betting operators and their service providers should maintain security measures commensurate with the sensitivity of the data involved, the available technology and its cost, and the risks involved, including adverse regulatory action or litigation. These steps can also provide a competitive edge in what is sure to be a crowded market.

The inevitable increase in online betting activity will likely involve security and privacy challenges and, therefore, individual users, employers, and mobile and online betting service providers should proactively take measures to protect against these issues.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice Teams. She can be reached at aclark@phillipslytle.com or (585) 238-2000 ext. 6466.